Cristela Johanneck

From: VisaRiskManager@visa.com
Sent: Tuesday, May 15, 2012 3:37 PM
To: visariskmanager@visa.com
Cc: visariskmanager@visa.com
Subject: Case Number US-2012-0244n-PA

Please be advised that this is one of many CAMS distributions related to this incident. You may or may not have impacted accounts in the previous or future distributions.

This is a PROACTIVE ALERT provided prior to confirmation of a compromise incident or substantiated forensic evidence of a breach.

Case Number: US-2012-0244n-PA
Date: May 15, 2012
Entity Type: Third Party Payment Processor (USA)

Suspected Data Elements at Risk:

Track 2: Yes

Fraud reported: Yes

Estimated Exposure Window: June 7, 2011 to August 31, 2011

Visa Fraud Control and Investigations is providing this Proactive Alert for potentially exposed customer transaction data that may have been put at risk. Visa has recently been notified by a third party processor that they have detected a security breach within their payment processing network. The network intrusion may have put accounts at risk of being stolen. A PCI DSS approved forensic company has been engaged and is working with the reporting entity. The U.S. Secret Service is also investigating this security breach.

The investigation is continuing and if additional accounts are determined to be at risk, additional CAMS alerts will be distributed.

These accounts are being provided as an early warning and will not be eligible for the Account Data Compromise Recovery (ADCR) or Data Compromise Recovery Solution (DCRS) recourse processes. A follow-up alert designated with the 'IC' suffix may be initiated and sent if the incident is confirmed and/or a network intrusion has been verified by the completion of a full forensic investigation. These account numbers may or may not be included in the follow-up alert.

The investigation is ongoing and this information may be amended as new details arise.

Please review your listed accounts at www.visaonline.com and take the necessary steps to prevent fraud and safeguard your cardholders. While assessing the appropriate action to take, you may want to review the compromised account best practices document located in the HELP section of Visa Risk Manager.

Disclaimer Information: This information is provided as an advisory service only and is intended solely for the addressee. Access to this information by any one else is unauthorized. If you are not the intended recipient, any disclosure, copying, or distribution is prohibited and may be unlawful. The author and Visa Inc. accept neither responsibility for the accuracy of this information nor any subsequent investigative action or otherwise taken by any individual member based on the information provided herein. This

advisory may be based on information provided to Visa Inc. by merchants, acquirers, third party processors and/or law enforcement. Visa Inc. accepts no responsibility for the information and advises Visa members to do their own verification to determine the accounts provided are at risk. Any action(s) taken by a Visa member based on this information is entirely at the member's own discretion.